QISS·ME

All-Silicon Quantum Key Distribution Circuits for Monolithic Datacenter Engines

Programm / Ausschreibung	Quantenforschung (QFTE), Quantenforschung und -technologie (QFTE), Quantenforschung und -technologie, Ausschreibung 2023, transnational	**Status**	laufend
Projektstart	01.03.2024	**Projektende**	28.02.2027
Zeitraum	2024 - 2027	**Projektlaufzeit**	36 Monate
Keywords	Quantum key distribution, Quantum communication, Silicon photonics, Quantum optics, Integrated circuits		

Projektbeschreibung

Cloud-Dienste erfreuen sich in jüngsten Jahren großer Beliebtheit. Innerhalb der zugrundeliegenden Datenzentren bleiben die Sicherheitsmaßnahmen jedoch weitgehend unberührt. Während externe Inter-Datacenter oder Metro-Core Verbindungen durch die Unterstützung von informationstheoretisch sicheren Verschlüsselungsmethoden wie etwa QKD als sicher gelten, werden Daten, die innerhalb des Perimeters dieser Rechenzentren gespeichert oder übertragen werden, ebenso als sicher angesehen. Diese Perimetersicherheit ist jedoch unzureichend, da internes Fehlverhalten grob vernachlässigt wird. Da 85% des gesamten Datenverkehrs innerhalb des Rechenzentrums verbleiben, kann ein solches Fehlverhalten jedoch schwerwiegende und weitreichende Schäden verursachen. Um zu einem Zero-Trust-Modell zu wechseln, bei dem keine Ressource des Datenzentrums von Natur aus vertrauenswürdig ist, ist es notwendig, die praktische Integration von QKD neu zu überdenken. Es erfordert vor allem eine disruptive Verkleinerung des QKD-Maßstabs – neben der Adressierung von Kostenzielen, um QKD nahtlos in Prozessor- und Speichereinheiten zu integrieren und gleichzeitig die enormen Datenraten von Datenzentren zu adressieren.
Hier verfolgt QISS•ME einen Chiplet-Ansatz, der eine System-in-Package Integration von QKD im Herzen von Rechenzentrum-Switches abzielt und damit das Abhören von Schnittstellensignalen des QKD-Systems praktisch unmöglich macht. Zu diesem Zweck wird QISS•ME einen monolithisch integrierten QKD-Sender für diskrete Variablen entwickeln, welcher Synergien mit der ausgereiften Silizium-Photonik Integrationsplattform nutzt, um eine weltweit erste Chiplet-QKD Implementierung auf einer Chipfläche von weniger als einem Quadratmillimeter zu realisieren. Eine vollständig auf Silizium ausgelegte Realisierung wird durch eine 1550-nm Silizium-Lichtquelle ermöglicht, die nahtlos mit einem Polarisationskodierer für das BB84 QKD Protokoll kombiniert wird. Dies ermöglicht die Generierung einer Schlüsselrate von 10 kb/s, um die Verschlüsselung der gesamten Link-Kapazität von 800 Gb/s von optischen Interconnects zu garantieren. Darüber hinaus wird eine Vereinfachung des QKD-Empfängers angestrebt, indem die Polarisationsdriftkompensation entlang des Faserübertragungskanals mit der Modulation der Quantenzustände am QKD-Sender integriert wird.
QISS•ME wird seine Chiplet-QKD Komponenten in diversen Anwendungsfällen evaluieren. Dazu gehören die Intra-Datacenter Kommunikation in Koexistenz mit klassischen Datenkanälen, sowie Datenzentren-Interconnects für High-Performance Computing über einen verlegten Faserkanal. Die Präsenz von Nvidia / Mellanox Technologies und Novarion im multi-

disziplinären Konsortium von QISS•ME stellt dabei sicher, dass die wissenschaftlichen Ziele des Projekts im Einklang mit industriellen Verwertungszielen stehen.

Abstract

Cloud services enjoy wide popularity among industries and professional users. Within the enabling datacenters, however, security measures remain largely untouched. Indeed, data stored or in transit within these information hotspots is deemed to be secure within the perimeter, while external datacenter interconnects or metro-core connections are supported by information-theoretic secure crypto primitives such as QKD. However, perimeter security is inadequate as it neglects internal misbehavior – an emerging threat that bears the potential to cause severe damage since 85% of total traffic remains within the datacenter.

Advancing to a zero-trust model, where no datacenter resource is inherently trusted, requires to rethink how QKD is practically introduced. It necessitates a disruptive down-scaling of the QKD footprint – next to addressing cost targets – to seamlessly integrate it with processors and storage, while further adhering to the massive data rates of datacenter environments.

This is where QISS•ME steps in with a chiplet approach that targets the system-in-package integration of QKD at the very heart of datacenter switches – rendering the signal interception at QKD interfaces as virtually impossible. Towards this direction, QISS•ME will develop a monolithic integrated discrete-variable QKD transmitter, drawing synergies from the mature silicon photonic integration platform to realize, for the first time, a chiplet QKD implementation with a sub-mm² footprint. An all-silicon implementation will be enabled through a 1550-nm silicon light source that is seamlessly blended with a polarization-encoder for BB84 QKD, to accommodate a secure-key rate of 10 kb/s for securing the whole link capacity of 800 Gb/s/lane optical interconnects. Moreover, simplification of the QKD receiver will be pursued through integrating polarization drift compensation along the fiber transmission channel with the quantum state preparation at the QKD transmitter. QISS•ME will demonstrate its all-silicon chiplet QKD components in various use-cases. These include East-West intra-datacenter transmission in co-existence with classical O-band channels and high-performance computing datacenter interconnects over field-installed fiber. The presence of Nvidia / Mellanox Technologies and Novarion in QISS•ME’s multi-disciplinary consortium will ensure alignment of the project‘s scientific goals with industry practices.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Novarion Systems GmbH